## REMARKS

Claims 1-21 are pending.

The Office Action mailed May 13, 2005 rejected claims 1-21 under 35 U.S.C. § 102(b) as anticipated by *Seid et al.* (U.S. 5,768,271). Applicant respectfully traverses the rejection of all claims, as the reference fails to disclose the features recited by the claims.

Independent claim 21 and dependent claims 2, 10, and 17 are not addressed in the Office Action's rejection of the claims. Applicant respectfully submits that the features recited by these claims are neither disclosed nor suggested by *Seid et al.*, and are thus allowable over *Seid et al.* Moreover, MPEP § 706.02(j) indicates that: "[i]t is important for an examiner to properly communicate the basis for a rejection so that the issues can be identified early and the applicant can be given fair opportunity to respond." Thus, the rejections of these claims should be withdrawn. Applicant further respectfully requests that, if a next Office Action maintains a rejection on these claims, that the next Action be made non-final, to better provide Applicant a "fair opportunity to respond."

Further, independent claim 1 recites, "a network system that resists denial of service attacks on **an access link to a destination host belonging to a virtual private network (VPN)**, said network system comprising: **one or more egress boundary routers having connections to an access network including the access link**, wherein said one or more egress boundary routers **transmit intra-VPN traffic toward the destination host from sources within the VPN and extra-VPN traffic toward the destination host from sources outside the VPN** within separate access network logical connections for intra-VPN and extra-VPN traffic, respectively; and a plurality of ingress boundary routers coupled to the one or more egress boundary routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic, such that denial of service attacks on said access link originating from sources

outside the VPN can be prevented." Independent claim 9 recites, "A network system, comprising: an access network having **an access link to a destination host belonging to a virtual private network (VPN)**, wherein said access network supports a first logical connection for intra-VPN traffic from sources within the VPN and a second logical connection for extra-VPN traffic from sources outside the VPN; **one or more egress boundary routers having connections to the access network**, wherein said one or more egress boundary routers **transmit intra-VPN traffic toward the destination host via the first logical connection and transmit extra-VPN traffic toward the destination host via the second logical connection**; and a plurality of ingress boundary routers coupled to the one or more egress boundary routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic, such that denial of service attacks on said access link originating from sources outside the VPN can be prevented." Independent claim 16 recites, "A method of protecting an **access link to a destination host belonging to a virtual private network (VPN)** against denial of service attacks, said method comprising: in an access network including the access link, providing a first logical connection for intra-VPN traffic from sources within the VPN and a second logical connection for extra-VPN traffic from sources outside the VPN; communicating, from **a plurality of ingress boundary routers to one or more egress boundary routers, intra-VPN and extra-VPN traffic destined for said destination host**, wherein said intra-VPN traffic and said extra-VPN traffic are transmitted utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic; **transmitting intra-VPN traffic from said one or more egress boundary routers toward the destination host via the first logical connection, and transmitting extra-VPN traffic from said one or more egress boundary routers toward the destination host via the second logical connection**, such that denial of service attacks on said access link originating from sources outside the VPN can be prevented."

In stark contrast, *Seid et al.* (per Abstract) is directed to congestion control in a network. Each virtual path VP in the network is allocated a positive guaranteed bandwidth (VP-CIR), and each virtual circuit (VC) on a VP is also allocated a bandwidth (VC-CIR) greater than or equal to zero. Packets of information to be transmitted over a VC are provided with a unique address field to identify the VCs and VPs associated with the VPN over which the packet of information will travel. Congestion control of the network is provided such that congestion control and management are carried out on a per VPN basis, and congestion outside of a VPN's logical domain does not affect the performance of the VPN.

In its rejection of claim 1, the Office Action cites Figs. 1-3, Figure 7, col. 4: 1-10, and col. 2: 56 – col. 3: 15 as disclosing the features recited by claim 1. However, Figure 7 is a block diagram showing the switching of virtual circuits within a node of the frame relay (FR) network of *Seid et al.* (in roles of FR connection switch, VP cross-connect, or VC switch, *see, e.g.*, col. 8: 13-18). In *Seid et al.*'s discussion of Figure 7, an "**ingress port** connection table" of a node of the FR network is shown at col. 8: 30-41, illustrating switching of VPs, thus illustrating *ingress and egress* ports with respect to a node in the network generally. (*See, e.g.*, col. 8: 13-57) There is no mention of any **boundary routers**, much less "one or more **egress boundary routers** having connections to an access network" including, as set forth in the preamble, the "access link to a destination host" as recited by claim 1. Further, there is no mention by *Seid et al.* of preventing "denial of service attacks on said access link originating from sources outside the VPN" as recited by claim 1.

The remaining cited portions of *Seid et al.* merely refer generally to providing a level of service for a VPN that is generally unperturbed by traffic generated by users outside of the VPN's logical domain. Nowhere does *Seid et al.* disclose or suggest "a network system that **resists denial of service attacks** on **an access link to a destination host belonging to a virtual**

**private network (VPN)**, said network system comprising: **one or more egress boundary routers having connections to an access network including the access link**, wherein said one or more egress boundary routers **transmit intra-VPN traffic toward the destination host from sources within the VPN and extra-VPN traffic toward the destination host from sources outside the VPN** within separate access network logical connections for intra-VPN and extra-VPN traffic, respectively" as recited by claim 1, nor does the Office Action contend that these specific features are disclosed by *Seid et al.* Thus, the rejection of claim 1 should be withdrawn.

For reasons similar to those stated previously with regard to claim 1, Applicant additionally submits that the rejection of independent claims 9 and 16 should be withdrawn.

The rejection of dependent claims 2-8, 10-15, and 17-20 should be withdrawn for at least the same reasons as their respective independent claims, and these claims are separately patentable on their own merits.

Therefore, the present application overcomes the objections and rejections of record and is in condition for allowance. Favorable consideration is respectfully requested. If any unresolved issues remain, it is respectfully requested that the Examiner telephone the undersigned attorney at (703) 425-8501 so that such issues may be resolved as expeditiously as possible.

Respectfully Submitted,

DITTHAVONG & CARLSON, P.C.

8/15/05
Date

Reg. No. 44,658

Margo Livesay, Ph.D.
Attorney/Agent for Applicant(s)
Reg. No. 41,946

10507 Braddock Road
Suite A
Fairfax, VA 22032
Tel. (703) 425-8501
Fax. (703) 425-8518